Colin, Carl

From: Wigmore, Steve [SWigmore@KSLAW.com]
Sent: Friday, September 29, 2006 10:38 AM
To: Colin, Carl
Subject: Proposed Examiner's Amendment for U.S. App. Ser. No. 09/665,019 - September 29, 2006

Examiner's AMENDMENT FOR Patent Application Serial No. 09/665,018

K&S File No. 05456.105007

Examiner Colin,

I appreciate you calling me and proposing this amendment. The Applicant agrees to all changes in the attached MS Word document.

Please send me a short note to confirm receipt of this e-mail and its MS Word attachment.

Thank you.

Best Regards,
Steve Wigmore
Reg. No. 40,447
(404)572-2884
<<App No 09-665-018 - Proposed Examiner Amendment - Sep 29 2006.doc>>

Examiner's AMENDMENT for Patent Application Serial No. 09/665,018

September 29, 2006

1. (Currently Amended) A computer-implemented process for assessing the vulnerability of a workstation to a security compromise, comprising the steps:

issuing a request for a scanner from a browser operating on the workstation to a network server via a computer network;

transmitting the scanner from the network server to the workstation via the computer network, the scanner installable within the browser and operative to complete a vulnerability assessment of the workstation to identify security vulnerabilities of the workstation that can compromise secure operation of the workstation on the computer network;

completing a repair operation by the scanner to address a security vulnerability identified by the scanner in response to completing the vulnerability assessment of the workstation;

generating workstation credentials derived from the scanner conducting the vulnerability assessment of the workstation, the workstation credentials comprising at least one of information about integrity of the workstation and a security posture of the workstation;

comparing the workstation credentials to a workstation policy;

authenticating a workstation for access to the network server by granting the workstation access to one or more services available on the network server if the workstation credentials derived from the scanner are in compliance with the workstation policy;

if access to the one or more services available on the network server is granted to the workstation because the workstation credentials are in compliance with the workstation policy, issuing a request for credentials associated with a user; receiving credentials associated with a user; and authenticating a user of the workstation for access to the network server after said authenticating the workstation for access to the network server by determining if the user is authorized to access the one or more services available on the network server through evaluating the credentials associated with the user; and

if the workstation credentials do not match the workstation security policy, then denying access to the one or more network services.

4. (Cancelled).

8. (Currently Amended) A computer-implemented process for authenticating a workstation requesting a software service, comprising the steps:

issuing a request for a scanner to a network server from a browser operating on the workstation;

transmitting the scanner and a workstation policy from the network server to the workstation via the computer network, the scanner installable within the browser and operative to generate workstation credentials by completing a vulnerability assessment of the workstation, the workstation credentials comprising at least one of information about integrity of the workstation and a security posture of the workstation;

completing a repair operation by the scanner to address a security vulnerability identified by the scanner in response to completing the vulnerability assessment of the workstation;

comparing the workstation credentials to the workstation policy on the workstation to determine whether the workstation should be granted access to the software service;

authenticating a workstation for access to the software service by granting the workstation access to the software service available on the network server if the workstation credentials derived from the scanner are in compliance with the workstation policy; and

if access to the software service is granted to the workstation because the workstation credentials are in compliance with the workstation policy, authenticating a user of the workstation for access to the software service after said authenticating the workstation for access to the software service by issuing a request for user authentication in order to determine if a user of the workstation is authorized to access the software service available on the network server; and

if the workstation credentials do not match the workstation security policy, then denying access to the software service.

11. (Currently Amended) A computer-implemented process for authenticating a workstation requesting a network service from a network server via a computer network, comprising the steps:

issuing a request for a scanner to the network server from a browser operating on the workstation;

transmitting the scanner from the network server to the workstation via the computer network, the scanner installable within the browser and operative to generate workstation credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network, the workstation credentials comprising at least one of information about integrity of the workstation and a security posture of the workstation;

completing a repair operation by the scanner to address a security vulnerability identified by the scanner in response to completing the vulnerability assessment of the workstation;

transmitting the workstation security credentials from the scanner to the network server via the computer network;

determining at the network server whether the workstation should be granted access to a network service of the network based on the workstation credentials;

authenticating a workstation for access to the network service by granting the workstation access to the network service if the workstation credentials derived from the scanner are in compliance with the workstation policy; and

if access is granted to the workstation for the network service because the workstation credentials are in compliance with the workstation policy, authenticating a user of the workstation for access to the network service after said authenticating the workstation for access to the network service by issuing a request for information relating to user authentication in order to determine if the user is authorized to access the network service; and

if the workstation credentials do not match the workstation security policy, then denying access to the network service.